UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/747,088	03/12/2001	John J. Stanaway JR.	STANAWAY 8-2	2312

22242	7590	05/05/2005

FITCH EVEN TABIN AND FLANNERY
120 SOUTH LA SALLE STREET
SUITE 1600
CHICAGO, IL 60603-3406

EXAMINER
KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 05/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2005*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

The new abstract filed on is accepted. Applicant's arguments/ amendments with

respect to amended claims 1, 10, & 15 and previously presented claims 2-9, 11-14, & 16-

18 filed on January 18, 2005 have been fully considered and therefore the claims are

rejected under new grounds. The examiner would like to point out that this action is

made final (See MPEP 706.07a).

Claim Rejections - 35 USC § 103

I.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

II.   Claims 1-3 and 10-11 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Sarkissian et al., United States Patent No. 6,771,646.

As per claims 1 and 10:

Sarkissian et al. substantially teach a security gateway for interfacing between

virtual private network data packets and corporate network packets, each data packet

comprising address information and payload, the security gateway comprising: a plurality

of protocol modules each for processing packets in accordance with a different network

protocols to access the payload (col. 8, lines 16-39 and col. 10, lines 25-37); memory for

storing protocol sequence information identifying which of the protocol modules is to

process each packet and the order of the processing (col. 8, line 5 – col. 10, line 51); a

protocol discriminator for receiving data packets and being responsive to the address

information of a received data packet for passing the received data packet to one or more

of the protocol modules, for processing thereby in the sequence identified by the protocol

sequence information to gain access to the payload (col. 9, line 61 – col. 10, line 51).

Not explicitly disclosed by Sarkissian et al. is the security gateway comprising

protocol modules for processing packets in accordance with different virtual private

network protocols. However, Sarkissian et al. mention examples of some different types

of protocols that are supported, where a VPN protocol is one of those mentioned.

Therefore, it would have been obvious to a person in the art at the time the invention was

made to modify the security gateway disclosed in Sarkissian et al. for the protocol

modules to process packets based on different VPN protocols. This modification would

have been obvious because a person having ordinary skill in the art, at the time the

invention was made, would have been motivated to do so since it is suggested by

Sarkissian et al. in col. 1, lines 51-55.

As per claim 2:

Sarkissian et al. substantially teach the security gateway as applied to claim 1

above. Furthermore, Sarkissian et al. teach the security gateway wherein each protocol

module receiving a data packet passes the received packet back to the protocol

discriminator upon completion of processing (col. 8, lines 29-col. 9, line 21).

As per claim 3:

Sarkissian et al. substantially teach the security gateway as applied to claim 2

above. Furthermore, Sarkissian et al. teach the security gateway wherein the protocol

discriminator selectively sends a data packet received from one of the protocol modules to another of the protocol modules (col. 8, lines 48-56).

As per claim 11:

Sarkissian et al. substantially teach the security gateway as applied to claim 10 above. Furthermore, Sarkissian et al. teach the method comprising accumulating the protocol sequence information during authentication of one or more communication request packets (col. 7, line 46 - col. 9, line 60).

III.   Claims 4-9 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sarkissian et al., United States Patent No. 6,771,646, as applied to claims 1 and 10 above, and further in view of Munger et al., United States Patent No. 6,502,135.

As per claim 4:

Sarkissian et al. substantially teach the security gateway as applied to claim 3 above. Not explicitly disclosed by Sarkissian et al. is the security gateway comprising a firewall interface to a corporate network and the protocol discriminator passes data packets to the firewall interface after processing by one or more of the protocol modules. However, Munger et al. teach firewalls for the protection of unauthorized access, receiving normal packets, and generate from these packets passed up to the Network (IP) layer. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the security gateway disclosed in Sarkissian et al. to have the protocol discriminator pass the data packets to the firewall interface after processing by one or more of the protocol modules. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since it is suggested by Munger et al. in col. 2, lines

51-63 and col. 11, lines 4-18.

As per claims 5 and 12:

Sarkissian et al. substantially teach the security gateway as applied to claim 1

above. Not explicitly disclosed by Sarkissian et al. is the security gateway wherein one

of the plurality of protocol modules processes virtual private network packets at a level 2

communication layer and another of the plurality of protocol modules processes virtual

private network packets at a level 3 communication layer.

However, Munger et al. teach six nodes on an Ethernet and the network is to be

split up into two private virtual networks with two sets of hardware addresses: one set for

the VPN and a second set for the second VPN. Therefore, it would have been obvious to

a person in the art at the time the invention was made to modify the security gateway

disclosed in Sarkissian et al. so that one of the protocol modules processes the VPN

packets at a level 2 communication layer and another protocol module processes the VPN

packets at a level 3 communication layer. This modification would have been obvious

because a person having ordinary skill in the art, at the time the invention was made,

would have been motivated to do so since it is suggested by Munger et al. in col. 23, lines

11-20.

As per claim 6:

Sarkissian et al. and Munger et al. substantially teach the security gateway as

applied to claim 5 above. Furthermore, Munger et al. teach a gatekeeper facilitates the

allocation and exchange of information needed to communicate securely, such as using

hopped IP addresses by using a secure communication function such as an IP hopping

function (col. 38, lines 53-60).

As per claim 7:

Sarkissian et al. and Munger et al. substantially teach the security gateway as

applied to claim 5 above. Furthermore, Munger et al. teach the packets have IP protocols

in the case of IPSEC (col. 40, lines 61-64).

As per claims 8 and 13:

Sarkissian et al. substantially teach the security gateway as applied to claim 1

above. Not explicitly disclosed by Sarkissian et al. is the security gateway comprising a

packet filter responsive to address information in packets presented thereto for selectively

granting and denying communication with the corporate network. However, Munger et

al. teach a packet filter rejecting hostile packets where hostile packets that match a header

will be rejected when the VPN software attempts to decrypt the header. Therefore, it

would have been obvious to a person in the art at the time the invention was made to

modify the security gateway disclosed in Sarkissian et al. so the packet filter can

selectively grant/deny communication with the corporate network based on address

information. This modification would have been obvious because a person having

ordinary skill in the art, at the time the invention was made, would have been motivated

to do so since it is suggested by Munger et al. in col. 30, lines 53-67 and col. 30, lines

26-28.

As per claims 9 and 14:

Sarkissian et al. and Munger et al. substantially teach the security gateway as

applied to claims 8 and 13 above. Furthermore, Munger et al. teach a small percentage of

hostile packets that pass the fast packet filter will be rejected when matching pairs are not

found in the active window or are active checkpoints (col. 30, lines 60-65).

IV.   Claims 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Munger et al., United States Patent No., 6,502,135, and further in view of Howard et al.,

United States Patent No., 6,353,886 and Sarkissian et al., United States Patent No.

6,771,646.

As per claim 15:

        Munger et al. substantially teach an algorithm governs the sequential selection of

IP address pairs; one sender and one receiver IP address (cot. 15, lines 27-31), the

combination of the algorithm, seed, and IP address block will be called a hopblock where

the send address and receive address of the IP header of each outgoing packet are filled

with the send and receive IP addresses generated by the algorithm (col. 15, lines 27-35), a

request is received by proxy server which checks its rules and determines that not VPN is

needed (col. 39, lines 61-66), the gate keeper has a rule to make a VPN which is

established between the client and the requested target where the gatekeeper would

provide the address of the destination to the proxy (col. 39, lines 42-52), and six nodes on

an Ethernet and the network is to be split up into two private virtual networks with two

sets of hardware addresses: one set for the VPN and a second set for the second VPN

(col. 23, lines 11-20), and the proxy server would receive the client's request and forward

it to gatekeeper. Gatekeeper would determine that no special VPN was needed, but that

the client was not authorized to communicate with non-VPN members. The gatekeeper

would reject the request, causing the proxy server to return an error message to the client

(col. 40, lines 4-13).

Not explicitly disclosed by Munger et al. is a set of rules and policies stored in the

security gateway so they are associated with the identity of the user. However, Howard et

al. teach policy records stored in the form of a certificate bound to a user. Therefore, it

would have been obvious to a person in the art at the time the invention was made to

modify the method disclosed in Munger et al. to use certificates incorporating policy

records in order to create an association between users and resources. This modification

would have been obvious because a person having ordinary skill in the art, at the time the

invention was made, would have been motivated to do so since it is suggested by Howard

et al. in col. 5, lines 2-65.

Also not explicitly disclosed by Munger et al. is the method wherein a packet is

received at the security gateway and the IP address assigned to the user is identified

based on the user identity and the IP address. However, Howard et al. teach that the IP

address is a part of the certificate. Therefore, it would have been obvious to a person in

the art at the time the invention was made to modify the method disclosed in Munger et

al. to for the IP address to be identified based on the user's identification information

contained in the certificate, including the IP address. This modification would have been

obvious because a person having ordinary skill in the art, at the time the invention was

made, would have been motivated to do so since it is suggested by Howard et al. in col. 7,

lines 3-13.

Finally, not explicitly disclosed by Munger et al. is processing received packets in

a plurality of protocol modules in accordance with the identified VPN protocols.

However, Sarkissian et al. teach different protocol modules for processing the packets

based on the identified protocol. Therefore, it would have been obvious to a person in the

art at the time the invention was made to modify the method disclosed in Munger et al.

for the protocol modules to process packets based on the identified VPN protocols. This

modification would have been obvious because a person having ordinary skill in the art,

at the time the invention was made, would have been motivated to do so since it is

suggested by Sarkissian et al. in col. 1 lines 51-55, col. 8 lines 16-39, and col. 10 lines

25-37.

As per claim 16:

Munger et al., Howard et al., and Sarkissian et al. substantially teach the method

of claim 15 above. Furthermore, Munger et al. teach the proxy server would receive the

client's request and forward it to gatekeeper. Gatekeeper would determine that no special

VPN was needed, but that the client was not authorized to communicate with non-VPN

members. The gatekeeper would reject the request, causing the proxy server to return an

error message to the client (col. 40, lines 4-13).

As per claim 17:

Munger et al., Howard et al., and Sarkissian et al. substantially teach the method

of claim 15 above. Furthermore, Munger et al. teach when matching pairs are not found

in the active window or are active checkpoints that hostile packets are rejected. Hostile

packets that match a header will be rejected when the software attempts to decrypt the

header. (col. 30, lines 61-67 and col. 40, lines 1-3).

As per claim 18:

Munger et al., Howard et al., and Sarkissian et al. substantially teach the method

of claim 15 above. Furthermore, Munger et al. teach access to secure site has been

requested, the proxy determines whether the user has sufficient security privileges to

access the site, proxy transmits a message to gatekeeper requesting that a virtual private

network be created, the gatekeeper creates hopblocks to be used by the computer and

secure target site for secure communication, the gatekeeper communicates these to user

computer, proxy returns to user computer the resolved address passed to it by the

gatekeeper using a secure administrative VPN (col. 38, lines 23-42).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the

advisory action. In no event, however, will the statutory period for reply expire later than

SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-

3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Albert Decady can be reached on (571) 272-3819. The fax phone number for

the organization where this application or proceeding is assigned is 703-872-9306.

Nadia Khoshnoodi
Examiner
Art Unit 2133
5/02/2005

NK

GUY LAMARRE
PRIMARY EXAMINER